IBM India/South Asia Blog

Building a next-gen Security Posture for the era of Hybrid Cloud & AI

Apr 5, 2021

Navigating a paradigm shift in enterprise security

Enterprises today operate in a ***globally segregated yet virtually connected business era*** . The large-scale adoption of digital technologies to support a remote workforce has simultaneously triggered a rise in cyberattacks targeting vulnerabilities across poorly secured devices and endpoints. With 25% of the workloads migrated to the cloud[*], enterprises today are managing security across complex IT landscapes spread across Public, Private or Hybrid Cloud environments leading to blind spots and increased risk. A recent study revealed India was the second most attacked country in Asia Pacific and it made up for 7% of all attacks observed in Asia in 2020.[**]

To navigate through complexities, organizations are embracing the shift from traditional analysis to synergetic Root Cause analysis spanning across people, process and technology. In addition, organizations are focused on adopting outcome-oriented security posture which provides a comprehensive and holistic security view across the organization, irrespective of the location and environment. The intent is not only to enhance the integrated security posture for the future, but to meet the underline expectations of the proverb that "***Prevention is better than a costly Cure" - very well justified considering an average statistical figure of $3.86Mn expenditure for handling data breach globally last year.***[***]

Analyzing the CHANGE in Technology landscape

As security threats continue to evolve, businesses have realized the critical need to invest wisely in group security initiatives. Any delays in strengthening enterprise security posture increases the risk of incurring a higher penalty. However, while making enterprise-wide technology decisions, most business leaders come across the following dilemma:

- Should the organization invest in buying different technology products which meet the needs of proactive and advanced security monitoring?
- Will there be seamless integration not only between various products but also the existing complex enterprise IT landscape?
- What could be the possible challenges and skills needed to manage various consoles and multiple vendors?
- Should the organization look for a partner, a trusted security advisor with the capability of deploying, managing and supporting all business requirements within "***one umbrella***"?

Staying ahead of the curve with a unified approach to security
Organizations are not only dealing with complex multicloud environment but also a variety of disconnected security tools from different vendors. The absence of unified visibility has conservatively cost organizations thousands of dollars in matter of hours due to unauthorized access to cloud assets. Given this risk and based on our experience, enterprises are seeking for solutions which provide comprehensive visibility across on-premises, SaaS and IaaS environments, detect threats in real time, eliminate manual tasks for analysts to focus on investigation and response and manage compliance easily through pre-built templates, reports etc.

IBM QRadar Security Information and Event Management (SIEM) platform helps organizations address the above challenges by detecting risks across users, protocols and applications. With QRadar Offense, the security analyst can view curated information related to the incident and extract additional details if required for conducting further investigation based on collected data including logs, network traffic packets and vulnerabilities. QRadar User Behavior Analytics combined with Machine Learning Analytics (ML) capabilities addresses this challenge and helps organizations to stay ahead in their security posture. With predictive modelling capabilities, a behavioural model for each individual is created based on their activity patterns. Any instance, outside of the normal pattern is immediately detected and flagged off by the system with the risk score. To assist security operations teams to do more, with greater accuracy, the QRadar Advisor with Watson app provides real time insights through incident and risk analysis, triage and response. Thereby, reducing the time spent investigating incidents from days and weeks to minutes or hours.

Some of the common use-cases for QRadar SIEM include:

- **Critical Data Protection** to help discover and protect against abnormal database connection attempts.
- **Advanced Persistent Threat management** to detect command control issues, correlate threat events with vulnerabilities and escalate them to perform acute offense detection.
- **Incident Response** which enables security analysts to see communication flow from infected hosts to curb the spread of data infection.
- **Meet compliance requirements** including stringent requirements for BFSI and healthcare industry. The platform enables monitoring for unauthorized or unexpected firewall configuration changes to allow access to critical business assets. For example, PCI requires all critical assets that contain "banking information" to communicate through an internal DMZ with no direct access to the outside world.
- **Risk and Vulnerability Management** to validate, assess and prioritize threats by correlating with asset

and vulnerability data.

Key Takeaways

Cyber risk will continue to be one of the greatest challenges for businesses in upcoming time. With network economy becoming the new norm and rising cost of data breach, businesses will need to relook at their cybersecurity approach to thrive and not just survive given the essential reliance on technology for partnering, culture, customer engagement, and more.

This blog is authored by Varun Vashisht, Cyber Security Solution Lead, TCS and Nikhil Bhavsar, WW Security Architect (GSI), IBM India

---

Sources: *IBM 4Q20 Report | IBM X-Force Threat Intelligence Index 2021 |***Ponemon Institute - 2020 Cost of Data breach report**

Blog Categories

Secure